10 August 2015

NORTH DAKOTA

Critical Infrastructure and Key Resources (CI/KR) Ticker

The North Dakota Open Source (CI/KR) Ticker a product of the North Dakota State and Local Intelligence Center (NDSLIC). It provides open source news articles and information on terrorism, crime, and potential destructive or damaging acts of nature or unintentional acts. Articles are placed in the (CI/KR) Ticker to provide situational awareness for local law enforcement, first responders, government officials, and private/public infrastructure owners.

NDSLIC Disclaimer

The (CI/KR) Ticker is a non-commercial publication intended to educate and inform. Further reproduction or redistribution is subject to original copyright restrictions. NDSLIC provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.

Table of Contents

North Dakota

(North Dakota) Production line catches fire at Grand Forks Simplot plant. The Simplot plant in Grand Forks, North Dakota sustained extensive damage August 1 after a fryer caught fire and spread to the roof of the building. Crews contained the incident and no injuries were reported. http://www.wday.com/news/north-dakota/3809331-update-production-line-catches-fire-grand-forks-simplot-plant

Regional

(National) Attorney: Dakota Dunes clinic cyber attack affects data for more than 13,000 patients. Siouxland Pain Clinic in Dakota Dunes notified over 13,000 patients July 31 that their personal and medical information may have been compromised in an attack on the clinic's server that occurred between March 26 and April 2. The clinic was notified of the breach June 26 and continues to investigate the incident. http://siouxcityjournal.com/news/attorney-dakota-dunes-clinic-cyber-attack-affects-data-for-more/article_d1550c3e-3371-5701-802e-5c90a9b6a9a2.html

National

Nothing Significant to Report

International

(International) Nuclear nightmare: Industrial control switches need fixing, now. Security researchers at Dragos Security discovered at least 11 vulnerabilities in control switches being used in industrial control systems (ICS) across multiple sectors that could allow an attacker to execute man-in-the-middle (MitM) attacks to cause control systems to shut down a plant or process or force an ICS into a hazardous state. Researchers believe that the attacks are being exploited in the wild, and that the vulnerabilities are made possible by poor authentication protocols and cryptographic integrity. http://www.zdnet.com/article/nuclear-nightmare-industrial-control-switches-need-fixing-now/

(International) China Read Emails of Top U.S. Officials. China's cyber spies have accessed the private emails of "many" top Obama administration officials, according to a senior U.S. intelligence official and a top secret document obtained by NBC News, and have been doing so since at least April 2010. http://www.nbcnews.com/news/us-news/china-read-emails-top-us-officials-n406046

Banking and Finance Industry

(International) SEC charges man with microcap fraud involving shares of Cynk Technology Corp. The U.S. Securities and Exchange Commission charged a Canadian man July 31 with allegedly using straw shareholders, foreign dummy corporations, and fake corporate officers worldwide to conceal his control of shares of Cynk Technology Corp., which he intended to liquidate when the stock's price increased.
http://www.sec.gov/news/pressrelease/2015-157.html

(National) Family indicted on $18M fraud. A former Tennessee State Representative and his 2 sons were indicted August 5 for using their company, First American Monetary Consultants Inc., to allegedly defraud over 300 people in at least 9 States out of $18 million by encouraging customers to buy gold and silver that they never completely received.
https://www.memphisdailynews.com/news/2015/aug/6/bates-family-indicted-on-18m-fraud/

(Texas) Feds: Austin man linked to $23M worth of counterfeit money. An Austin man was indicted August 4 for role in a counterfeiting scheme in which he allegedly forged and distributed U.S. currency worth up to $23 million from March to July. Two other suspects were recently found guilty in connection to counterfeiting U.S. currency in the Austin area.
http://kxan.com/2015/08/05/feds-austin-man-linked-to-23m-worth-of-counterfeit-money/

(International) GameOver Zeus gang leader engaged in espionage: Researchers. Officials from FBI, Fox-IT, and Crowdstrike released analysis revealing that in addition to using the GameOver Zeus malware to steal about $100 million from banks, the cybercriminal ring used botnets to commit cyberespionage against

various countries, including members of the Organization of the Petroleum Exporting Countries (OPEC).
http://www.securityweek.com/gameover-zeus-gang-leader-engaged-espionage-researchers

Chemical and Hazardous Materials Sector

Nothing Significant to Report

Commercial Facilities

(Tennessee) New horror at the movies: Man with axe, pellet gun goes berserk. Three individuals were injured after a man armed with a pellet gun and a hatchet released pepper spray at audience members inside a Tennessee movie theater before being shot at and killed by police August 5. Authorities unarmed a hoax device found in the man's backpack and believe the individual suffered significant psychiatric problems.
http://www.cbsnews.com/news/antioch-tennessee-movie-theater-shooting/

Communications Sector

(International) Android device makers promise monthly security fixes. Google, Samsung, and LG announced plans to begin issuing monthly security patches for Android devices, citing the operating system's (OS) increased targeting from cybercriminals. The first large update includes a patch for the Stagefright vulnerability, which can compromise a device via a specially crafted multimedia message (MMS).
http://www.computerworld.com/article/2960512/security/android-device-makers-promise-monthly-security-fixes.html

(International) 80 vulnerabilities found in iOS in 2015, 10 in Android. Secunia released findings from a report on security vulnerability trends for the first 7 months of 2015 revealing an increase of "extremely critical" and "highly critical" threats, a trending increase in zero-day exploits, and a total of 80 reported vulnerabilities in Apple's iOS operating system (OS) versus 10 in Android devices. Researchers cited Apple's control of its OS and patch cycle as the cause for higher number if iOS vulnerabilities.

http://news.softpedia.com/news/80-vulnerabilities-found-in-ios-in-2015-10-in-android-488676.shtml

Critical Manufacturing

(National) **Mazda recalls 193k CX-9 crossovers over corroded suspension.** Mazda issued a recall for 193,484 model years 2007 – 2014 CX-9 vehicles due to an issue in which water leaking into front suspension ball joints may cause corrosion, resulting in a loss of steering control.
http://www.autoblog.com/2015/08/05/mazda-cx9-suspension-recall/

(National) **Tesla Issues Fix After Researchers Hack a Model S and Bring It to a Stop.** Tesla Motors said on Thursday it has sent a software patch to address security flaws in the Model S sedan that could allow hackers to take control of the vehicle.
http://www.nbcnews.com/tech/security/tesla-issues-fix-after-researchers-hack-model-s-bring-it-n405251

(International) **Gone in less than a second.** A security researcher unveiled a wallet-sized device, called Rolljam, that can be hidden underneath a vehicle and can intercept codes used to unlock most cars and garage doors employing rolling codes, by jamming the signal and replaying the next rolling code in the sequence. The developer previously created a device that was able to intercept communication between certain vehicles and the OnStar RemoteLink mobile application to locate, unlock, and remotely start a vehicle.
https://threatpost.com/gone-in-less-than-a-second/114154

Defense/ Industry Base Sector

(International) **Unauthorized repairs sideline Navy's three newest fast-attack subs.** U.S. Navy officials reported August 5 that the USS John Warner, the USS Minnesota, and the USS North Dakota fast-attack submarines are to be held in port at the Yokosuka Naval Base in Japan due to concerns over pipe elbows used to send steam to the submarine turbines, after General Dynamics Electric Boat determined that three elbows supplied by a subcontractor required additional testing and repair due to unauthorized and undocumented weld repairs performed on the parts.

http://www.military.com/daily-news/2015/08/06/unauthorized-repairs-sideline-navys-three-newest-subs.html

Emergency Services

(Illinois) **Governor asks FEMA for storm-related assessment help.** The governor of Illinois issued a State disaster proclamation the week of August 3 for 23 counties that were severely impacted by a series of storms in June and July, and has requested the assistance of the Federal Emergency Management Agency (FEMA) with damage assessments and funding for the counties. http://www.pantagraph.com/news/local/rauner-asks-fema-for-storm-related-assessment-help/article_a09d31ba-74cc-5676-8210-2020b2fb09a1.html

(California) **Company: California oil spill from pipeline break could be 40 percent larger than estimated.** Texas-based Plains All American Pipeline released preliminary documents August 5 stating that a pipeline which ruptured May 19 near Santa Barbara, California, may have spilled up to 143,000 gallons of crude oil, up from the original 101,000-gallon estimate. http://www.foxbusiness.com/markets/2015/08/05/company-california-oil-spill-from-pipeline-break-could-be-40-percent-larger/

(Missouri) **Gunfire erupts in Ferguson on anniversary of Michael Brown's killing.** A day of peaceful vigils to mark the one-year anniversary of Michael Brown's shooting death turned ugly late Sunday when protesters threw rocks and bottles at officers, and police critically injured a man who they say fired at them. http://www.cnn.com/2015/08/10/us/ferguson-protests/index.html

Energy

(Michigan) **Storms pummel state, produce tornado.** A line of thunderstorms in southeastern Michigan cut power to approximately 92,000 DTE Energy customers August 2 and 63,000 customers remained without service August 3 while crews worked to restore service by August 4. The storm caused flooding which prompted the closure of northbound Interstate 75 ramp at Interstate 94 in Detroit and the southbound Interstate 75 ramp to eastbound Interstate 94. http://www.detroitnews.com/story/news/local/michigan/2015/08/02/metro-detroit-tornadoes-possible/31023811/

(Rhode Island; Massachusetts) **More than 100,000 residents without power throughout RI and SE MA.** National Grid reported 109,220 power outages due to severe weather in Rhode Island, as well as 10,000 in Massachusetts August 4. The Massachusetts Bay Transportation Authority (MBTA) also reported a downed tree and an electrical malfunction which delayed MBTA commuter rail service. http://wpri.com/2015/08/04/thousands-without-power-throughout-the-state/

(Oklahoma) **Oklahoma acts to limit earthquake risk at oil and gas wells.** Oklahoma regulators announced August 3 new requirements demanding a 38 percent reduction in wastewater disposal for 23 injection wells in a 40-mile earthquake zone between Oklahoma City and Stillwater in response to a growing trend of earthquakes linked to increased hydraulic fracturing. http://www.nytimes.com/2015/08/05/us/oklahoma-acts-to-limit-earthquake-risk-at-oil-and-gas-wells.html?_r=0

(International) **Trend Micro uncovers attacks on Internet-connected petrol stations.** Trend Micro experts investigating data attacks against automated gas tank systems using a custom international honeypot dubbed GasPot presented research at Black Hat 2015 which found 12 pump identifications, 4 pump modifications and 2 denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks against the systems from February – July 2015. Researchers suspect that several hacktivist groups, including the Iranian Dark Coders Team and the Syrian Electronic Army, were behind the attacks, a majority of which targeted the U.S. http://www.infosecurity-magazine.com/news/trend-micro-uncovers-attacks-on/

(Alaska) **Alaska oil and gas producer that took State tax credits faces fraud charges.** The U.S. Securities and Exchange Commission announced August 6 charges against Knoxville-based Miller Energy Resources that the company allegedly inflated values of oil and gas properties acquired in Cook Inlet in 2009 by over $400 million, leading to fraudulent financial reports regarding the company's net income and total assets. A former and current executive were also implicated in the civil claims filed August 6. https://www.adn.com/article/20150806/alaska-oil-and-gas-producer-took-state-tax-credits-faces-accounting-fraud-charges

Food and Agriculture

(Iowa) Bird flu quarantines being lifted. Iowa officials reported August 4 that 69 of the 77 bird flu quarantine zones in the State were in the process of being lifted, and only 8 other farms remain under quarantine in Adair, Clay, Sioux, Webster, and Wright counties.
http://www.cbs2iowa.com/news/features/top-stories/stories/Bird-Flu-Quarantines-Being-Lifted-180369.shtml

Government Sector (including Schools and Universities)

(California) California wildfires torch 134,000 acres – and counting. Crews in California reached 12 percent containment August 4 of the 60,000-acre Rocky Fire burning in Lake, Yolo, and Colusa counties that led to evacuation orders for more than 13,000 people. Firefighters worked to contain a total of 21 wildfires in the State that have burned over 134,000 acres collectively.
http://www.cnn.com/2015/08/03/us/california-wildfires/

Information Technology and Telecommunications

(International) DNS server attacks being using BIND software flaw. Security researchers from Sucuri reported that attackers have begun exploiting a denial-of-service (DoS) flaw in all versions of BIND 9 open-source Domain Name System (DNS) software that was patched the week of July 27. The company confirmed that two clients in different sectors had experienced attacks.
http://www.computerworld.com/article/2955290/security/dns-server-attacks-begin-using-bind-software-flaw.html

(International) Chinese VPN used by APT actors relies on hacked servers. Security researchers at RSA analyzed a Chinese virtual private network (VPN) service dubbed "Terracotta" and found that the service has at least 31 hacked Windows server nodes worldwide in hospitality, government organizations, universities, technology services providers, and private firms. Researchers have observed compromised servers running the Gh0st Remote Administration Tool (RAT), the Mitozhan trojan, and the Liudoor Backdoor, among others.
http://www.securityweek.com/chinese-vpn-used-apt-actors-relies-hacked-servers

(International) Updated DGA Changer malware generates fake domain stream. Researchers from Seculert published findings from a report revealing that the DGA Changer downloader malware now has the capability to generate a stream of fake domains once it determines that it is being run in a virtual environment, the first reported instance of malware generating fake domain generation algorithms (DGA).
https://threatpost.com/updated-dga-changer-malware-generates-fake-domain-stream/114159

(International) BLEKey device breaks RFID physical access controls. Researchers at Black Hat 2015 released details from a number of proof of concept attacks highlighting the weaknesses in the Wiegand protocol used in radio-frequency identification (RFID) readers and other proximity card devices, which they were able exploit by using a device dubbed BLEKey to read cleartext data sent from card readers to door controllers to clone cards or send data to a mobile application that can unlock doors remotely at any time.
https://threatpost.com/blekey-device-breaks-rfid-physical-access-controls/114163

Public Health

(National) Data of 4 million patients lost in MIE hacking. The Indiana Attorney General announced that an estimated 1.5 million State residents and 3.9 million individuals from 11 healthcare providers and 44 radiology clinics nationwide may have been impacted by a May breach of Medical Informatics Engineering and its subsidiary NoMoreClipboard's networks. Officials continue to investigate the attack, which allowed hackers to gain access to patients' personal and medical information.
http://news.softpedia.com/news/data-of-4-million-patients-lost-in-mie-hacking-488319.shtml

Transportation

(International) MH370 Mystery: Officials Confirm Fragment Is From Missing Flight. The airplane fragment that washed up on an island last week was a piece of Malaysia Airlines Flight 370, the Malaysian prime minister confirmed Wednesday. The fragment — a 6-foot-long, barnacle-encrusted wing flap — was discovered on July 29 by a crew cleaning the beach on Reunion Island, a French territory in the Indian Ocean off the southern tip of Africa. **http://www.nbcnews.com/storyline/missing-jet/mh370-mystery-officials-confirm-fragment-missing-flight-n404546**

Water and Dams

(Colorado) **Colorado Mine Spill: Toxic Wastewater Leak Far Exceeds First Estimates.** A spill that sent toxic water seeping from an abandoned Colorado gold mine and turned a river orange. Original estimates claimed around a million gallons of wastewater had spilled. The EPA said Sunday that 3 million gallons of wastewater had spilled from the mine, and the sludge was still flowing. The EPA said that health risks to humans and aquatic life were not yet clear. http://www.nbcnews.com/news/us-news/colorado-mine-spill-toxic-wastewater-leak-far-exceeds-first-estimates-n407091

North Dakota Homeland Security Contacts

To report a homeland security incident, please contact your local law enforcement agency or one of these agencies: North Dakota State and Local Intelligence Center: 866-885-8295(IN ND ONLY); Email: ndslic@nd.gov; Fax: 701-328-8175 State Radio: 800-472-2121; Bureau of Criminal Investigation (BCI): 701-328-5500; North Dakota Highway Patrol: 701-328-2455; US Attorney's Office Intel Analyst: 701-297-7400; Bismarck FBI: 701-223-4875; Fargo FBI: 701-232-7241.

To contribute to this summary or if you have questions or comments, please contact:

Darin Hanson, ND Division of Homeland Security dthanson@nd.gov, 701-328-8165